

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 03-224047

(43)Date of publication of application : 03.10.1991

(51)Int.Cl. G06F 12/14
G06K 19/073

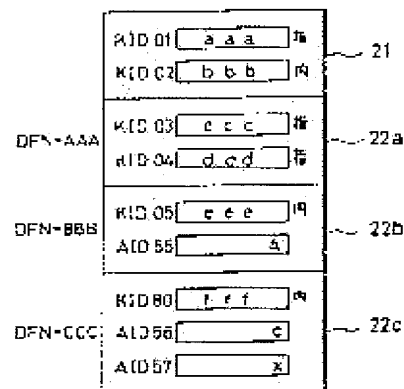
(21)Application number : 02-017924 (71)Applicant : TOSHIBA CORP
(22)Date of filing : 30.01.1990 (72)Inventor : IIJIMA YASUO

(54) PORTABLE ELECTRONIC DEVICE

(57)Abstract:

PURPOSE: To decide the propriety of accesses to a memory while keeping the security by deciding whether the key data used for confirmation belongs to a common data file or an application data file and then clearing the result of confirmation at selection of applications if the key data belongs to the application data file.

CONSTITUTION: A data memory consists of a common data file 21 which is used in common by all application and plural application data files 22a - 22c which are used individually by each application. Then it is decided whether they key data used for confirmation belongs to the common data file or the application data file. If the key data belongs to the latter data file, the result of confirmation of the application data file is cleared at selection of applications. Thus it is possible to decide the propriety of accesses to the data memory based on the result of confirmation while keeping the security among applications.



⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑫ 公開特許公報(A)

平3-224047

⑤ Int. Cl.⁵

識別記号

庁内整理番号

④ 公開 平成3年(1991)10月3日

G 06 F 12/14
G 06 K 19/073

3 2 0 C

7737-5B

6711-5B G 06 K 19/00

P

審査請求 未請求 請求項の数 1 (全8頁)

⑬ 発明の名称 携帯可能電子装置

⑭ 特 願 平2-17924

⑮ 出 願 平2(1990)1月30日

⑯ 発 明 者 飯 島 康 雄 神奈川県川崎市幸区柳町70番地 株式会社東芝柳町工場内

⑰ 出 願 人 株 式 会 社 東 芝 神奈川県川崎市幸区堀川町72番地

⑱ 代 理 人 弁理士 鈴 江 武 彦 外3名

明 細 書

1. 発明の名称

携帯可能電子装置

2. 特許請求の範囲

少なくともメモリと、このメモリに対してアクセスを行なう制御素子を有し、選択的に外部とのデータの授受を行なうもので、かつ前記メモリは、全てのアプリケーションで共通にアクセス対象となる第1の領域と、各アプリケーション個々に使用される少なくとも1つの第2の領域とに分割されているとともに、これら第1および第2の領域内に少なくとも1つのキーデータを有する携帯可能電子装置であって、

本装置の起動後は前記第1の領域のみアクセス対象とする手段と、

外部より前記第2の領域のうち1つを選択する選択情報を受信する第1の受信手段と、

この第1の受信手段により受信した選択情報に基づいて対応する第2の領域を選択的にアクセス可能とならしめる手段と、

少なくとも第1のデータを第1のキーデータにより暗号化された第1の暗号データを受信する第2の受信手段と、

第1のデータを選択された第2の領域に対応する第1のキーデータにより暗号化して第2の暗号データを生成する暗号化手段と、

この暗号化手段により生成した第2の暗号データと前記第2の受信手段により受信した第1の暗号データとを比較する比較手段と、

この比較手段の比較結果に基づいて前記メモリに対するアクセスの可否を判定する手段と、

新たに第2の領域のうち1つが選択されたときに前記比較結果の基となる第1のキーデータが前記第1の領域内に存在するか第2の領域内に存在するかを判断する手段と、

この判断の結果、第2の領域内に存在すると判断されるとき、前記比較結果の肯定結果を否定結果とする手段と

を具備したことを特徴とする携帯可能電子装置。

3. 発明の詳細な説明

〔発明の目的〕

(産業上の利用分野)

本発明は、たとえば消去可能な不揮発性メモリおよびCPUなどの制御素子を有するIC(集積回路)チップを内蔵した、いわゆるICカードと称される携帯可能電子装置に関する。

(従来技術)

最近のICカードに要求される機能として、外部装置(ICカードを取扱う端末装置など)との相互認証機能が提案されている。この場合、外部装置との間で必ず相互認証を行わなければ、アクセスが不可というようなアクセス制御方式がある。

(発明が解決しようとする課題)

この場合、ICカードが多目的用途になるにつれ、アプリケーションごとに認証用のキーデータを有することが考えられるが、このとき例えばアプリケーションAにおいて認証処理を施した結果がアプリケーションBを運用する際にも使用可

能であると、アプリケーション間のセキュリティ分離が困難である。

そこで、本発明は、各アプリケーションごとに異なる認証用のキーデータを有し、かつアプリケーション間のセキュリティを保ちつつ、認証結果によりメモリに対するアクセスの可否を決定することが可能な携帯可能電子装置を提供することを目的とする。

〔発明の構成〕

(課題を解決するための手段)

本発明は、少なくともメモリと、このメモリに対してアクセスを行なう制御素子を有し、選択的に外部とのデータの授受を行なうもので、かつ前記メモリは、全てのアプリケーションで共通にアクセス対象となる第1の領域と、各アプリケーション個々に使用される少なくとも1つの第2の領域とに分割されているとともに、これら第1および第2の領域内に少なくとも1つのキーデータを有する携帯可能電子装置であって、本装置の起動後は前記第1の領域のみアクセス対象とする手

段と、外部より前記第2の領域のうち1つを選択する選択情報を受信する第1の受信手段と、この第1の受信手段により受信した選択情報に基づいて対応する第2の領域を選択的にアクセス可能とならしめる手段と、少なくとも第1のデータを第1のキーデータにより暗号化された第1の暗号データを受信する第2の受信手段と、第1のデータを選択された第2の領域に対応する第1のキーデータにより暗号化して第2の暗号データを生成する暗号化手段と、この暗号化手段により生成した第2の暗号データと前記第2の受信手段により受信した第1の暗号データとを比較する比較手段と、この比較手段の比較結果に基づいて前記メモリに対するアクセスの可否を判定する手段と、新たに第2の領域のうち1つが選択されたときに前記比較結果の基となる第1のキーデータが前記第1の領域内に存在するか第2の領域内に存在するかを判断する手段と、この判断の結果、第2の領域内に存在すると判断されると、前記比較結果の肯定結果を否定結果とする手段とを具備している。

(作用)

認証に使用したキーデータがコモンデータファイル(第1の領域)のものか、アプリケーションデータファイル(第2の領域)のものかを判断し、もしアプリケーションデータファイルのものであれば、アプリケーション選択時に認証結果をクリアするものである。これにより、各アプリケーションごとに異なるキーデータを持たせ、このキーデータで認証を行ない、その結果によりメモリに対するアクセスの可否を決定することによって成立するセキュリティ確保がアプリケーション間のセキュリティを保ちつつ行なえる。

(実施例)

以下、本発明の一実施例について図面を参照して説明する。

第6図は本発明に係る携帯可能電子装置としてのICカードを取扱う端末装置の構成例を示すものである。すなわち、この端末装置8は、ICカード1をカードリーダー・ライター2を介してCPUなどからなる制御部3と接続可能にするとともに、

制御部3にキーボード4、CRTディスプレイ装置5、プリンタ6およびフロッピーディスク装置7を接続して構成される。

ICカード1は、ユーザが保持し、たとえば商品購入などの際にユーザのみが知得している暗証番号の参照や必要データの蓄積などを行なうもので、第5図にその機能ブロックを示すように、リード・ライト部11、暗証設定・暗証照合部12、および暗号化・復号化部13などの基本機能を実行する部分と、これらの基本機能を管理するスーパーバイザ14とで構成されている。リード・ライト部11は、後述するデータメモリ16に対してデータの読出し、書込み、あるいは消去を行なう機能である。暗証設定・暗証照合部12は、ユーザが設定した暗証番号の記憶および読出禁止処理を行なうとともに、暗証番号の設定後にその暗証番号の照合を行ない、以後の処理の許可を与える機能である。暗号化・復号化部13は、たとえば通信回線を介して制御部3から他の端末装置へデータを送信する場合の通信データの漏洩、偽造を

防止するための暗号化や暗号化されたデータの復号化を行なうものである。スーパーバイザ14は、カードリーダー・ライター2から入力された機能コードもしくはデータの付加された機能コードを解釈し、前記基本機能のうち必要な機能を選択して実行させる機能である。

これらの諸機能を発揮させるために、ICカード1は例えば第4図に示すように、制御素子(たとえばCPU)15、データメモリ16、プログラムメモリ17、およびカードリーダー・ライター2との電気的接触を得るためのコンタクト部18によって構成されており、これらのうち破線内の部分(制御素子15、データメモリ16、プログラムメモリ17)は1つのICチップ(あるいは複数のICチップ)で構成されてICカード本体内に埋設されている。

プログラムメモリ17は、たとえばマスクROMで構成されており、前記各基本機能を実現するサブルーチンを備えた制御素子15の制御プログラムなどを記憶するものである。

データメモリ16は、各種データの記憶に使用され、たとえばEEPROMなどの消去可能な不揮発性メモリで構成されている。

データメモリ16は、たとえば第3図に示すように、全てのアプリケーションで共通に運用する1つのコモンデータファイル(以降、CDFと略称する)21と、各アプリケーション個別に運用する複数のアプリケーションデータファイル(以降、ADFと略称する)22a, 22b, 22cとによって構成されており、各ADF22a, 22b, 22cには、それぞれデータファイル名(DFN)が付与されている。

そして、第3図の例においては、CDF21内には、キーデータ番号K1D01で示される指定用キーデータaaa、およびキーデータ番号K1D02で示される内部キーデータbbbが含まれ、またDFN=AAAで示されるADF22aには、キーデータ番号K1D03で示される指定用キーデータccc、およびキーデータ番号K1D04で示される指定用キーデータddd

が含まれる。DFN=BBBで示されるADF22bには、キーデータ番号K1D05で示される内部キーデータeee、およびエリア番号A1D55で示されるデータエリアが含まれており、特にデータエリアはADF22b内の内部キーデータによる認証処理で認証が確認されるとアクセス可能という属性情報(A)が付与されている。また、DFN=CCCで示されるADF22cには、キーデータ番号K1D08で示される内部キーデータfff、エリア番号A1D56で示されるデータエリア、およびエリア番号A1D57で示されるデータエリアが含まれている。特に、エリア番号A1D56で示されるデータエリアは、CDF21内の内部キーデータによる認証処理で認証が確認されるとアクセス可能という属性情報(C)が付与されており、エリア番号A1D57で示されるデータエリアは、CDF21内の内部キーデータまたはADF22c内の内部キーデータによる認証処理で認証が確認されるとアクセス可能という属性情報(X)が付与さ

れている。

ここに、指定用キーデータとは、端末装置8がICカード1を認証するためのキーデータであり、内部キーデータとは、ICカード1が端末装置8を認証するためのキーデータである。

次に、第1図を用いてICカード1の動作概要を説明する。ICカード1は、端末装置8から第2図(a)の電文を受信すると、その機能コードから選択的に第1図(a)の相互認証準備フローを実行する。これらの処理は、制御素子15によりプログラムメモリ17内のプログラムにしたがって行われる。すなわち、まずADFが選択済か否かを、内部RAM(制御素子15内のRAM)中の選択ADF固有情報を参照することにより確認する。このとき、選択済でなければ、データメモリ16上のCDF21より、入力電文中のキーデータ番号(KID)を見つけ、また、選択済であれば、CDF21内とさらに選択済ADF内よりKIDを見つける。もし、この時点で見付からなければエラーステータス出力する。なお、通

常は起動時にはCDF21が自動的に選択されている。

キーデータ番号(KID)を見つければ、対応するキーデータを内部的にリードし、正常か否かをチェックする。このとき、正常でなければエラーステータス出力する。正常であれば、電文中の乱数情報Aと該キーデータを内部RAMの所定領域に記憶しておく。次に、この乱数情報Aと、カード発行時にセットされるカード固有の番号、それと、データメモリ16内にあらかじめ初期値として記憶されているカード乱数情報とにより所定のアルゴリズムに従って乱数情報Bを生成し、これを新たなカード乱数情報として書き換えておく。

次に、再度ADFが選択済か否かを確認し、選択済でなければ、CDF21より内部キーデータのKIDを見つけ、選択済であれば、CDF21内と更に選択済ADF内よりKIDをみつける(ADFが優先的に対象となる)。もし見つからなければ、エラーステータス出力する。見つか

ったなら、対応するキーデータを内部的にリードし、正常か否かをチェックする。このとき、正常でなければエラーステータス出力する。

さて、正常であれば、先に生成した乱数情報Bを見つけた内部キーデータを暗号キーとして暗号化し、その結果を認証情報C2Xとして内部RAMの所定領域に記憶しておく。そして、内部キーデータのKIDと乱数情報Bを出力し、本フローを終了する。

このフローにより、端末装置8とICカード1との間の相互認証における乱数情報と、キー指定情報を共有することができる。

次に、第2図(b)の電文を受信すると、その機能コードから選択的に第1図(b)のフローを実行する。すなわち、まず先に説明した相互認証準備コマンドが実行済であるか否かを確認して、否であればエラーステータス出力する。

実行済であれば、次に入力された電文中の認証情報C2と、先に内部RAM上に記憶しておいた認証情報C2Xとを比較し、一致していれば一致

フラグをオンし、そうでなければオフにする。このとき、一致フラグは、ADFの認証結果を示すADF対応一致フラグと、CDFの認証結果を示すCDF対応一致フラグとがあり、内部キーデータが属するものがADFかCDFかにより、ADF対応一致フラグかCDF対応一致フラグかをオン、オフする。次に、先に内部RAM上に記憶しておいた乱数情報Aを、指定用キーデータを暗号キーとして暗号化し、その結果を認証情報C1Xとして先の一致フラグの結果と共に出力し、本フローを終了する。

このフローにより、端末装置8との相互認証が可能となる。

次に、第2図(c)の電文を受信すると、その機能コードから選択的に第1図(c)のADF選択フローを実行する。すなわち、まず電文中のDFNがICカード1のデータメモリ16に登録されているか否かを確認し、見つからなければエラーステータス出力する。

もし見つければ、先のC2/C2Xの一致フ

グのうち、A D F 対応一致フラグをオフする。次に、指定 D F N に対応する固有情報を内部 R A M に保持し、正常終了ステータスを出力する。

次に、第 2 図 (d) で示すリードコマンド電文または第 2 図 (e) で示すライトコマンド電文を受信すると、その機能コードから選択的に第 1 図 (d) のフローを実行する。すなわち、まず A D F が選択済か否かを判断し、選択済でなければ、C D F 2 1 内より入力電文中のエリア番号 (A I D) を見つけ、選択済であれば、選択済 A D F 内と C D F 2 1 内より A I D を見つける。このとき、見つからなければ、エラーステータスを出力する。見つければ、対応して記憶されているエリアの属性情報を参照し、先の一致フラグを確認する必要があるか否かを判断する。もし、必要であれば、それが A D F 対応一致フラグか C D F 対応一致フラグか、または、そのどちらでも良いかを判断する。

もし、A D F 対応一致フラグが必要、もしくはどちらでも良いという場合であれば、A D F 対応

一致フラグを参照し、オンとなっているか否かをチェックする。もしオフであればエラーステータスを出力する。

また、C D F 対応一致フラグが必要、もしくはどちらでも良いという場合であれば、C D F 対応一致フラグを参照し、オンとなっているか否かをチェックする。もしオフとなっていればエラーステータスを出力する。

そして、電文中の機能コードにより、対応するリードまたはライト処理を施し、その処理結果を出力する。

次に、たとえば第 3 図のようなキーデータおよびエリアの構成に対する I C カード 1 の動作を説明する。第 3 図においては前述した通りであり、この状態で、A D F 選択を行わない場合の相互認証には、指定用キーデータには K I D 0 1 のキーデータが使用され、内部キーデータには K I D 0 2 のキーデータが使用される。

また、D F N = A A A により A D F 2 2 a が選択された状態では、指定用キーデータには K I D

0 3 または K I D 0 4 のキーデータ、または K I D 0 1 のキーデータが使用され、内部キーデータとして K I D 0 2 のキーデータが使用される。

同様に、D F N = B B B により A D F 2 2 b が選択された状態では、指定用キーデータには K I D 0 1 のキーデータが使用され、内部キーデータには K I D 0 5 のキーデータが使用される。

さて、A D F 2 2 b 内の A I D 5 5 のエリアに対してアクセスするためには、このエリアの属性は A D F 2 2 b 内の内部キーデータを必要とするようになっている。よって、A D F 2 2 b を選択した後の相互認証を行わなければならない。仮に、相互認証後に A D F 2 2 b を選択すると、この相互認証に使用する内部キーデータは K I D 0 2 のキーデータとなるからである。

また、A D F 2 2 c 内の A I D 5 6 のエリアに対してのアクセスには、このエリアの属性が C D F 2 1 内の内部キーデータを必要とするようになっている。よって、C D F 内部のキーデータ K I D 0 2 を用いた相互認証後に A D F 2 2 c を

選択し、エリアにアクセスしなければならない。したがって、C D F 対応一致フラグがオンになっていればアクセス可能である。

また、A I D 5 7 のエリアについては、内部キーデータを必要としていないので、C D F 2 1 内のキーデータ K I D 0 2 を用いた相互認証後に A D F 2 2 c を選択しても、その逆、つまり A D F 2 2 c を選択した後に A D F 2 2 c 内のキーデータ K I D 0 8 によって相互認証を行なった後でもアクセス可能とならしめることになる。

したがって、特に最初に A D F 2 2 b を選択し、相互認証を実行した後、次に A D F 2 2 c を選択した場合、A I D 5 7 のエリアに対してアクセスはできない状態となる。

このように、認証に使用したキーデータがコモンデータファイル (C D F) のものか、アプリケーションデータファイル (A D F) のものかを判断し、もしアプリケーションデータファイルのものであれば、アプリケーション選択時にアプリケーションデータファイルの認証結果をクリアする

ものである。これにより、各アプリケーションごとに異なるキーデータを持たせ、このキーデータで認証を行ない、その結果によりデータメモリに対するアクセスの可否を決定することによって成立するセキュリティ確保がアプリケーション間のセキュリティを保ちつつ行なえる。

【発明の効果】

以上詳述したように本発明によれば、各アプリケーションごとに異なる認証用のキーデータを有し、かつアプリケーション間のセキュリティを保ちつつ、認証結果によりメモリに対するアクセスの可否を決定することが可能な携帯可能電子装置を提供できる。

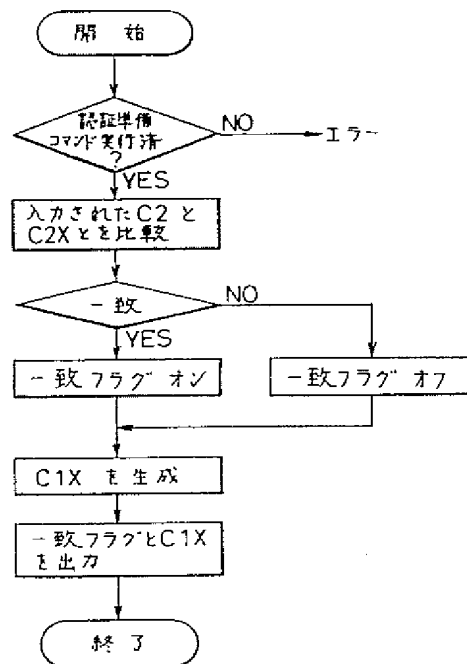
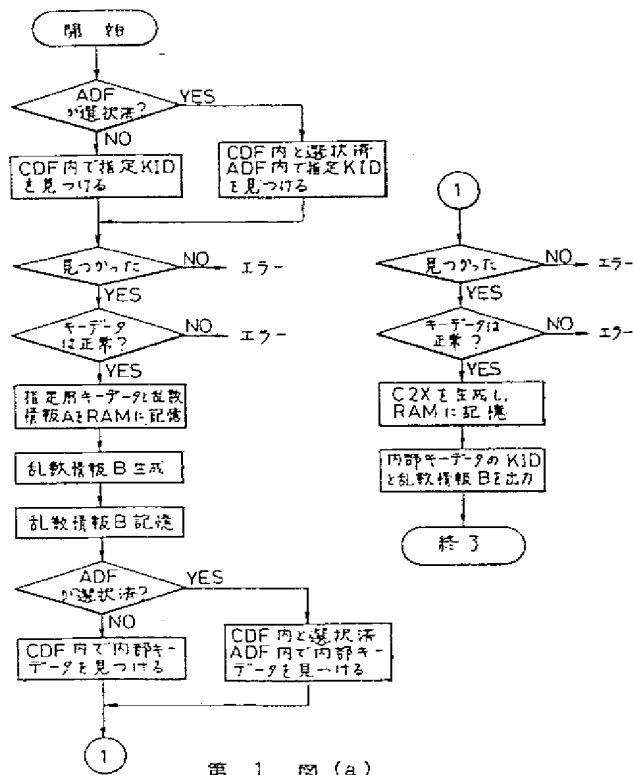
4. 図面の簡単な説明

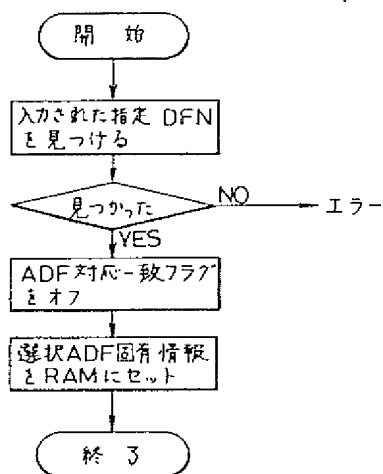
図は本発明の一実施例を説明するためのもので、第1図はICカードの動作概要を説明するフローチャート、第2図はICカードに入力される各種コマンド電文フォーマット例を示す図、第3図はデータメモリのファイル構造を示す図、第4図はICカードの概略構成を示すブロック図、第5図

はICカードの機能ブロックを示す図、第6図は端末装置の構成を示すブロック図である。

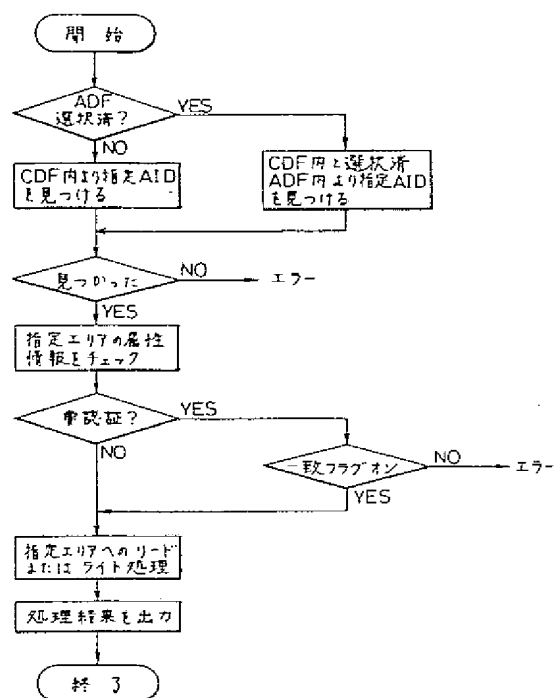
1 …… ICカード（携帯可能電子装置）、8 …… 端末装置、15 …… 制御素子、16 …… データメモリ（不揮発性メモリ）、17 …… プログラムメモリ、21 …… コモンデータファイル（CDF、第1の領域）、22a、22b、22c …… アプリケーションデータファイル（ADF、第2の領域）。

出願人代理人 弁理士 鈴江武彦

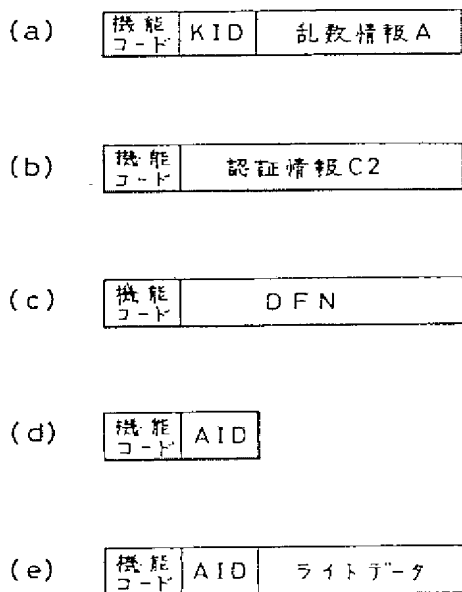




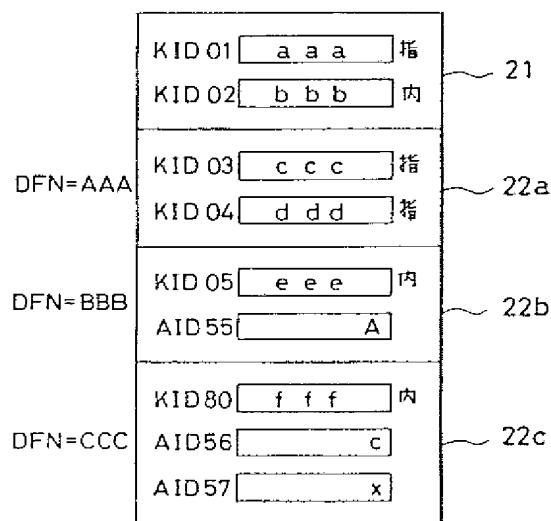
第 1 図 (c)



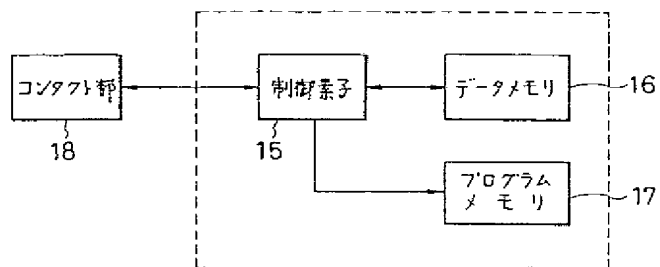
第 1 図 (d)



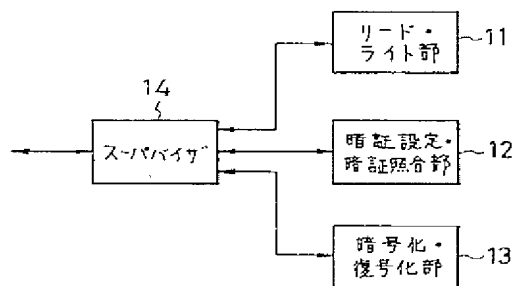
第 2 図



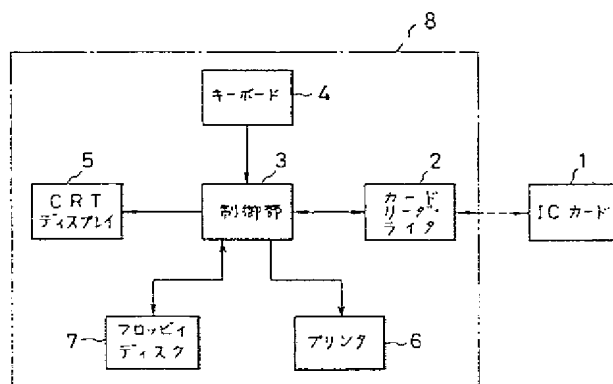
第 3 図



第 4 図



第 5 図



第 6 図